CHAPTER 16

Computer Networking

16. Computer Networking

16.1 Overview

A Computer Network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links (data connections). The connections between nodes are established using either cable media or wireless media.

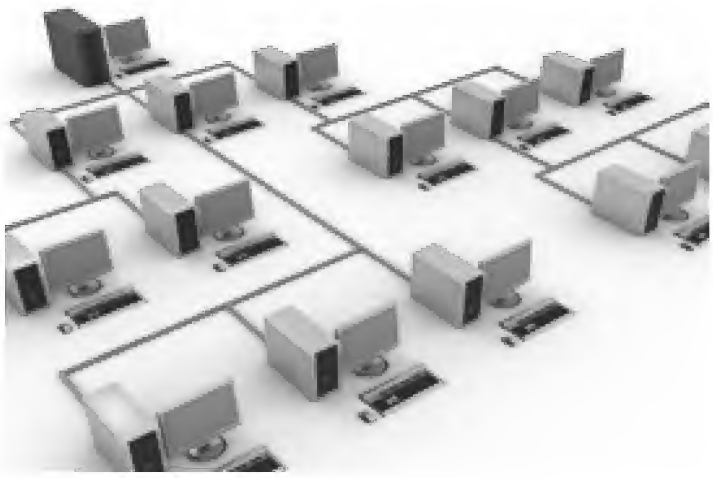


Figure 16.1 – Computer Network

In other words a computer network is basically a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered as a computer network.

16.2 Basics of Computer Networking

The major basic components of Computer Networking can be classified as under:

1. Network Connections or Links
2. Network Protocols – Layers of Networking
3. Network Types
4. Network Topology
5. Network Strategy
6. Organizational Scope of Network
7. Network Bandwidth Classification

16.2.1 Network Connections/Links

The transmission media (often referred as the physical media) used to link devices to form a computer network primarily includes electrical cable (Ethernet, power line), optical fiber (fiber-optic communication) and radio waves (wireless networking). Major types are enlisted below:-

- A widely adopted family of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables.
- Wireless LAN standards (e.g. those defined by IEEE 802.11) use radio waves, or others use infrared signals as a transmission medium.
- Power line communication uses a building's power cabling to transmit data.

The various connections possible are given below.

16.2.1.1 Wired Physical Network Link

Twisted Pair Wire

A type of cable that consists of two independently insulated wires twisted around one another. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. While twisted-pair cable is used by older telephone networks and is the least expensive type of local-area network (LAN) cable, most networks contain some twisted-pair cabling at some point along the network

Figure 16.2 – Twisted Pair Wire

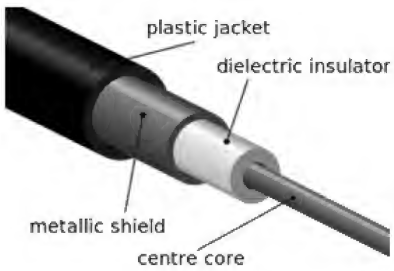


Figure 16.3 – Co-Axial Cable

Co-axial Cable

A type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference.

Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for computer networks, such as Ethernet. Although more expensive than standard telephone wire, it is much less susceptible to interference and can carry much more data.

Optical Fiber


Figure 16.4 – Optical Fiber

This technology uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Fiber optics has several advantages over traditional metal communications lines:

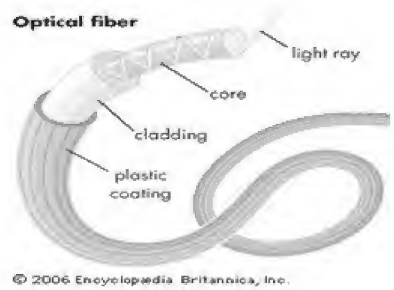


Figure 16.5 – Optical Fiber

a) Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.

b) Fiber optic cables are less susceptible than metal cables to interference.

c) Fiber optic cables are much thinner and lighter than metal wires.

d) Data can be transmitted digitally (the natural form for computer data) rather than analogically

T1 & T3 Lines

The Tier 1 or T1 is a digital line that is usually private and used for businesses. The businesses that use T1 tend to have more control over their line than other options. It also is considered more reliable. Its speeds are roughly the same or lower than Cable and DSL, reaching up to 1.5Mbitps upload and download. Though upload/download isn't amazing; still T1 lines do well for smaller businesses.

Tier 3 is a bigger, faster, more expensive version of T1. It can get up to 44Mbitps upload and download speeds. It is great for medium/large businesses, as it provides a good deal of bandwidth.

T1 and T3 are two common types of leased lines used in telecommunications. Both T1 lines and T3 lines are reserved circuits that operate over either copper or fiber optic cables.

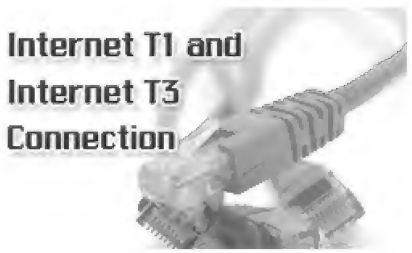


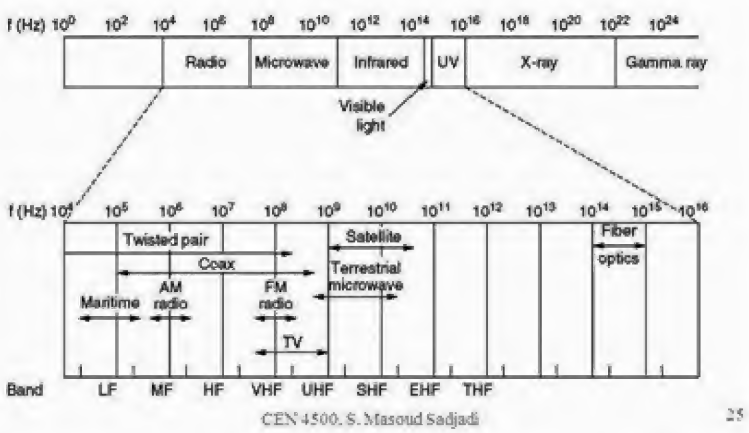
Figure 16.6 – T1 & T3

16.2.1.2 Wireless Links

Modern age has given rise to information junkies – people normally want to be online all the time. For these mobile users, traditional wire media is of no use. They need to get their hits of data for laptop, palmtop or mobiles without being tethered to the terrestrial communication infrastructure. For all such users, wireless communication is the answer.

Use of Electromagnetic (EM) Spectrum

When electrons move, they create EM waves that can propagate via space (even in vacuum). When an antenna of appropriate size is attached to an electrical circuit, the EM waves can be broadcast efficiently & received by a receiver some distance away. This is the basic principle of all wireless communication.



Band	Frequency range	Wavelength range
Extremely low frequency (ELF)	< 3 kHz	>100 km
Very low frequency (VLF)	3 - 30 Hz	10 - 100 krn
Low frequency(LF)	30 - 300 kHz	1 - 10 km
Medium frequency (MF)	300 kHz - 3 MHz	100m - 1km
High frequency (HF)	3 - 30 MHz	10 - 100m
Very high frequency (VHF)	30 - 300 MHz	1 - 10m
Ultra high frequency (UHF)	300 MHz - 3 GHz	10cm - 1m
Super high frequency (SHF)	3 - 30 GHz	1 - 10cm
Extremely high frequency (EHF)	30 - 300 GHz	1mm - 1cm

Figure 16.7 - EM Spectrum & Frequency Bands

The radio, microwave, infrared & visible light portions of the spectrum can all be used for transmitting information. Ultraviolet light, X rays & Gamma rays would be even better but due to their complex nature & harm to living beings, not used.

The various types of wireless links are explained below in detail:

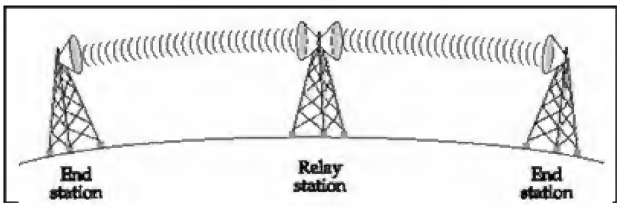


Figure 16.8 – Microwave Communication

Terrestrial Microwave

Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.Microwave radio is used in broadcasting and telecommunication transmissions because, due to their short wavelength, highly directional antennas are smaller and therefore more practical.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other.

Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it.

One disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can. Typically, microwaves are used in television news to transmit a signal from a remote location to a television station from a specially equipped van.

Communication Satellite

Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

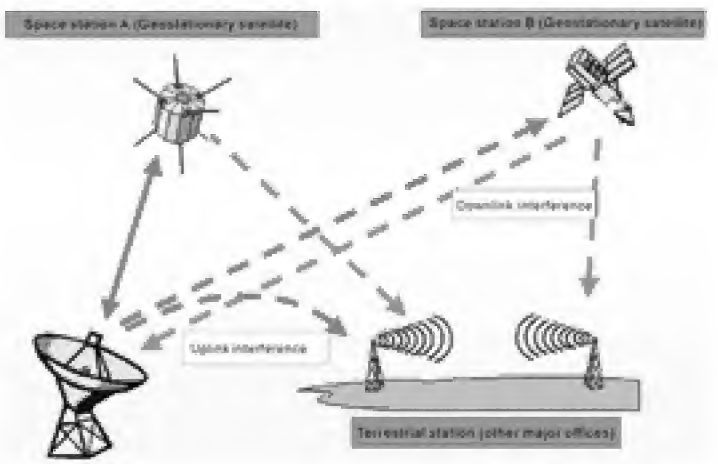


Figure 16.9 – Satellite Communication

A communications satellite is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder; it creates a communication channel between a source transmitter and a receiver(s) at different locations on Earth. Communications satellites are

used for television, telephone, radio, internet, and military applications.

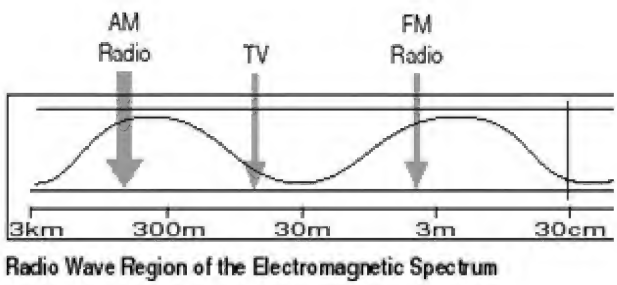


Figure 16.10 – Radio Waves

Radio Waves

Wireless local area networks use a high-frequency radio technology and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area.

Radio waves are a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared light. Radio waves have frequencies from 300 GHz to as low as 3 kHz, and corresponding wavelengths ranging from 1 millimeter (0.039 in) to 100 kilometers (62 mi).

Artificially generated radio waves are used for fixed and mobile radio communication, broadcasting, radar and other navigation systems, communications satellites, computer networks and innumerable other applications.

Cellular Network

The cellular systems divide the region covered into multiple geographic areas or cells. Each area or cell has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

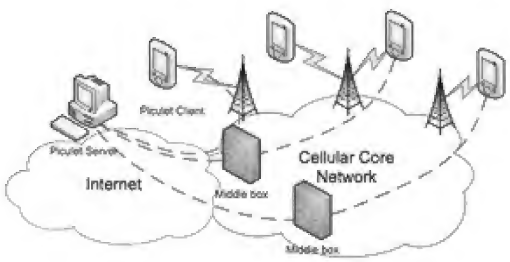


Figure 16.11 – Cellular Network

The cellular network is typically distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. This base station provides the cell with the network coverage which can be used for transmission of voice, data and others.

In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Infra-Red

IR (Infrared) wireless is the use of wireless technology in devices or systems that convey data

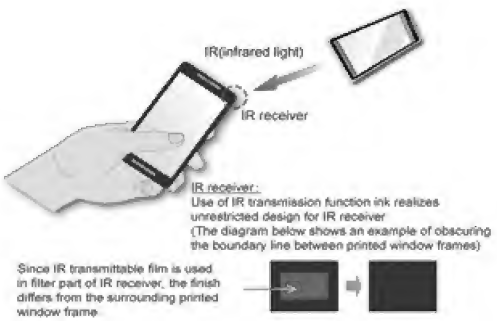


Figure 16.12 – Infra Red

through infrared (IR) radiation.

IR wireless is used for short- and medium-range communications and control. Some systems operate in line-of-sight mode; this means that there must be a visually unobstructed straight line through space between the transmitter (source) and receiver (destination). Other systems operate in diffuse mode, also called scatter mode. This type of system can function when the source and destination are not directly visible to each other.

Main characteristics of this kind of wireless optical communication is physically secure data transfer, line-of-sight (LOS) and very low bit error rate (BER) that makes it very efficient.

The main reason for using IR has been wireless data transfer over the **"last one meter"** using point-and-shoot principles. Thus, it has been implemented in portable devices such as mobile telephones, laptops, cameras, printers, medical devices, TV remote controls.

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the band from 2.4 to 2.485 GHz from fixed and mobile devices, and building personal area networks (PANs). It can connect several devices, overcoming problems of synchronization.

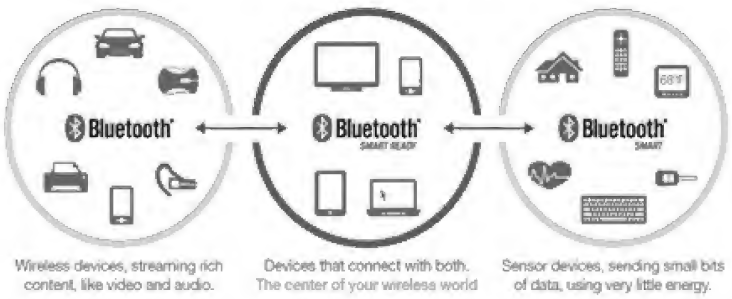


Figure 16.13 - Bluetooth

Bluetooth is basically a standard wire-replacement communications protocol primarily designed for low-power consumption, with a short range based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other. Range is power-class-dependent, but effective ranges vary in practice.

Figure 16.14 - WiFi

WiFi

Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices

to connect to the network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF radio bands.The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.

Many devices can use Wi-Fi, e.g. personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Such an access point **(or hotspot)** has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage range can vary.

RFID (Radio Frequency Identification)

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader.

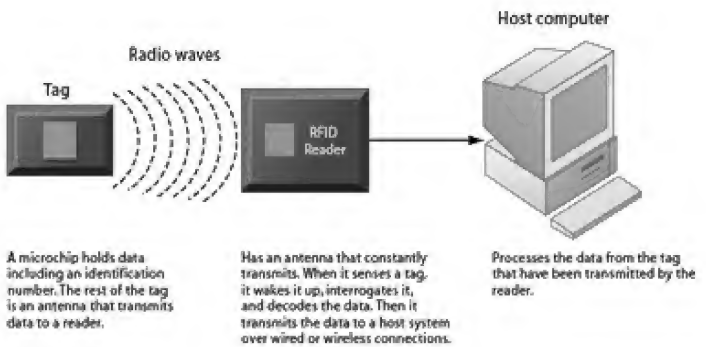


Figure 16.15 - RFID

RFID tags are used in many sectors like logistics/shopping malls, manufacturing assembly lines, etc.

GPRS (General Packet Radio Service)

GPRS is a data service technology that enables 2G telecommunication networks to provide services other than voice calls. These services include access to email, multimedia messaging, and a somewhat limited access to the internet. It was mostly used by old mobile sets. GPRS communicates with terrestrial cellular towers.

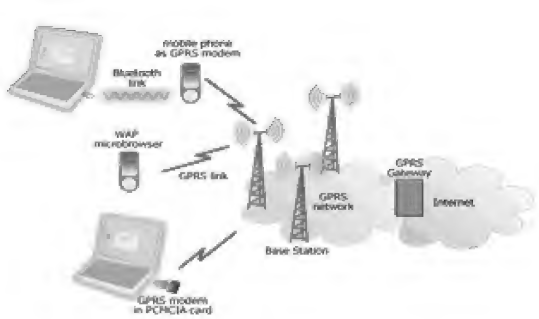


Figure 16.16 - GPRS

GPS (Global Positioning System)

GPS is simply navigation that your phone can use to get you from place to place through a wireless provider's network.

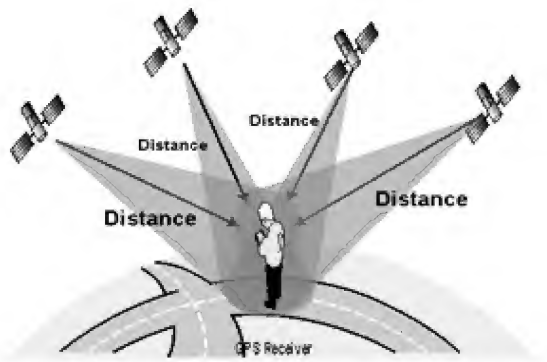


Figure 16.17 - GPS

GPS is global position system, which uses timings from satellites to determine location. It has no relation to GSM or GPRS, except in the case of A-GPS (assisted GPS) which might use mobile data provided via GSM/GPRS to quickly get data needed to calculate your position that would take 1-2 minutes to receive from the GPS satellites directly.

WiMAX (Worldwide Interoperability for Microwave Access)

It is a family of wireless communications standards designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations.

WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.

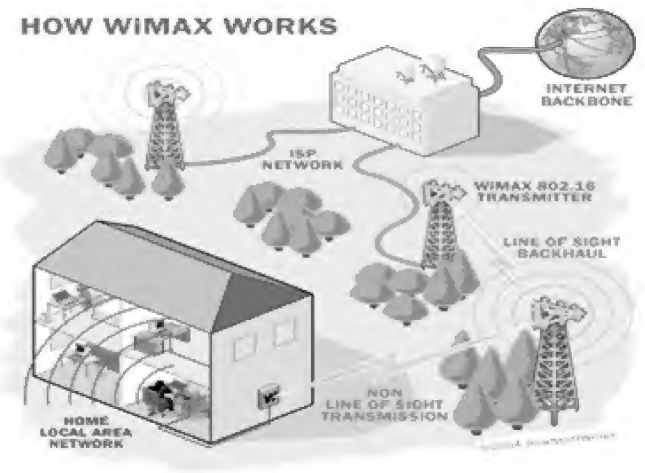


Figure 16.18 - WiMAX

The various bandwidth classifications are shared below for a quick reference:

Frequency range	Application	Frequency range	
500 kHz to 30 MHz	AM Radio	500 MHz to 2 GHz	Mobile phones
80-110 MHz	FM Radio	2.4, 5 GHz	Wireless LAN
100 MHz to 1 GHz	TV	1-100 THz	Infrared
500 MHz to 40 GHz	Microwave	10^{14} to 5 x 10^{14} Hz	Visible light
1-50 GHz	Satellite communication	5 x 10^{14} to 10 Hz	Ultraviolet

Medium	Copper UTP	Coaxial cable	Microwave links	Satellite links	Fibre optic cables	Wireless LAN	Mobile phones
Frequency band	0-100 MHz	100 KHz to 750 MHz	500 MHz to 20 GHz	1 GHz to 50 GHz	100 THz to 1000 THz	2.4, 5 GHz unlicensed bands	900 MHz - 2G 2 GHz - 3G

Figure 16.19 – Bandwidth Classifications

USEFUL TIP

Nowadays most common communication network that we use is Cellular due to the rise of mobile phones. It is the most flexible and efficient protocol which offers best mobility with least interference & power usage.

QUICK REVIEW

- What are the types of Physical communication links?
- What are the types of Wireless Communication links?
- What is the difference between Microwave & Satellite communication?

16.2.2 Network Protocols – 4 layers of Networking

The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks. It is commonly known as TCP/IP, Transmission Control Protocol (TCP) and the Internet Protocol (IP).TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination. This functionality is organized into **four abstraction layers** which are used to sort all related protocols according to the scope of networking involved.

Layer 1: Network Access Layer

Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

Layer 2: Internet Layer

Internet layer packs data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination.

Layer 3: Transport Layer

The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Layer 4: Application Layer

Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), etc.

USEFUL TIP

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. However a newer model called OSI (Open System Interconnection) is now used more.

QUICK REVIEW

- How many layers are there in TCP/IP Model?
- What is the difference between Network Access layer & Application Layer?

16.2.3 Network Types

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Major kinds of networks based on size & span are:

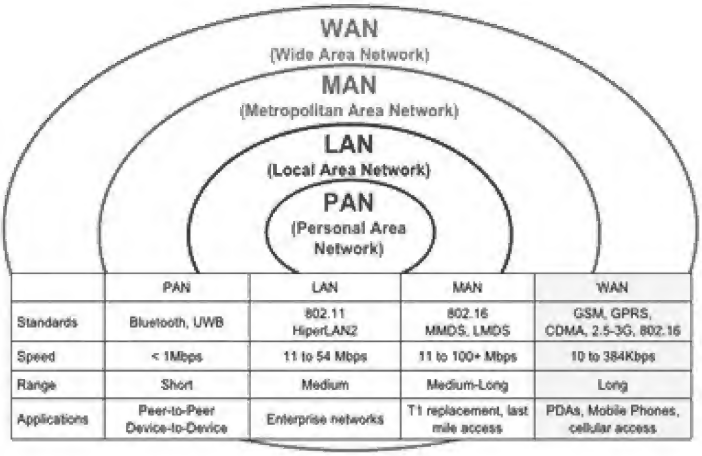
PAN (Personal Area Network)

Such networks let devices communicate over the range of a person. It used for data transmission among devices such as computers, telephones and personal digital assistants. For example Bluetooth, Embedded Medical Device Operations, RFID

LAN (Local Area Network)

It is privately owned network that operates within & nearby a single building like home (Home

Network), office or factory. LANs are widely used to connect PCs & consumer electronics to let them share resources (e.g. printers) & exchange information. e.g. WiFi



	PAN	LAN	MAN	WAN
Standards	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, cellular access

Figure 16.20 – Network Types

Wireless LANs (WLAN)

WLAN are very popular these days at places, where it is too much trouble to install cables. Compared to wireless networks, wired LANs exceed them in all dimensions of performance. It is just easier to send signals over a wire or through a fiber than through the air. The topology of many wired LANs is built from point to point links. The most common type of wired LAN is known as Ethernet (IEEE 802.3)

MAN (Metropolitan Area Network)

Such a network covers a city. E.g. Cable TV network, WiMAX

WAN (Wide Area Network)

Such a network spans a large geographical area, often a country or continent.e.g. VPN (Virtual Private Network, ISP (internet Service Provider), Cellular Telephone Network, 3G, Satellite Communication.

Overall comparison of Network types in a nutshell is depicted below:

USEFUL TIP

Under PAN, there is a new kind of network kind called BAN (Body Area Network) specifically targeting smart wearable devices.

QUICK REVIEW

- What are the various kinds of Network?
- What is the difference between MAN & WAN?
- What kind of network is a Bluetooth connection?

16.2.4 Network Topology

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer

network. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

Overall we have following 6 types of Network Topologies:

Bus Topology

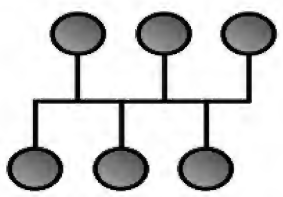


Figure 16.21 – Bus Topology

In local area networks where bus topology is used, each node is connected to a single cable, by the help of interface connectors. This central cable is the backbone of the network and is known as the bus (thus the name). A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient.

Because the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. Additionally, because only one cable is utilized, it can be the single point of failure.

Star Topology

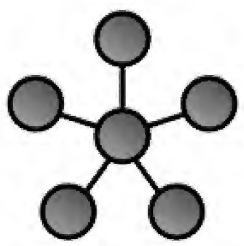


Figure 16.22 - Star Topology

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node with the help of the hub. In Star topology every node (computer workstation or any other peripheral) is connected to a central node called hub, router or switch. The switch is the server and the peripherals are the clients.

All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The primary disadvantage of the star topology is that the hub represents a single point of failure.

Ring Topology

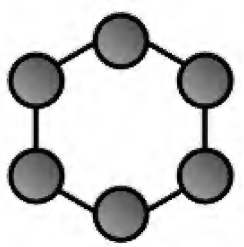


Figure 16.23 – Ring Topology

A network topology is set up in a circular fashion in such a way that they make a closed loop. This way data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link.

In a ring topology, there is no server computer present; all nodes work as a server and repeat the signal. The disadvantage of this topology is that if one node stops working, the entire network is affected or stops working.

Tree Topology

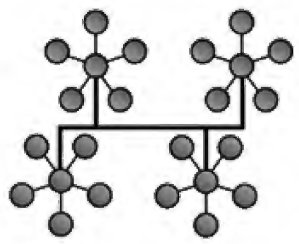


Figure 16.24 – Tree Topology

A tree topology is essentially a combination of bus topology and star topology. The nodes of bus topology are replaced with standalone star topology networks. This results in both disadvantages of bus topology and advantages of star topology.

For example, if the connection between two groups of networks is broken down due to breaking of the connection on the central linear core, then those two groups cannot communicate, much like nodes of a bus topology. However, the star topology nodes will effectively communicate with each other.

Hybrid Topology

Hybrid networks use a combination of any two or more topologies, in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected.

Two common examples for Hybrid network are: star ring network and star bus network.

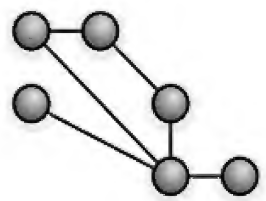


Figure 16.25 – Mesh Topology

Mesh Topology

A mesh network is a network topology in which each node relays data for the network. All mesh nodes cooperate in the distribution of data in the network.

Mesh networks can relay messages using either a flooding technique or a routing technique using self-healing algorithms. Self-healing allows a routing-based network to operate when a node breaks down or when a connection becomes unreliable. As a result, the network is typically quite reliable, as there is often more than one path between a source and a destination in the network.

USEFUL TIP

With the advent of wireless smart devices and internet boom, most of the latest networks would be based on Mesh type of network giving best efficiency.

QUICK REVIEW

- What are the types of Network Topology?
- What is the difference between Star & Ring Topology?

16.2.5 Network Strategy

types are explained below:-

Terminal Server

A central computer (Terminal Server) stores all your important programs, which are necessary for users. You connect your applications by End-machine (other than the Terminal Server). There's no need to install your programs on all your machines, a solution with Terminal Server, you only need a computer with monitor, keyboard, mouse and network adapter.

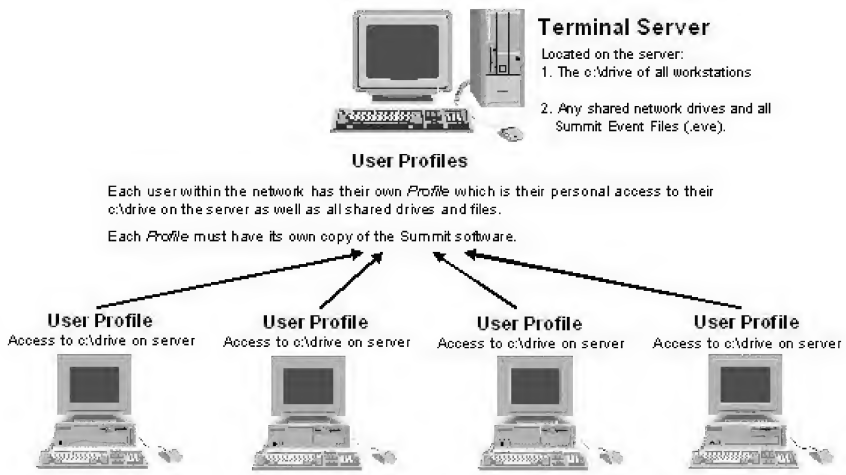


Figure 16.26 Terminal Server

In a terminal server network, processing power is centralized in one large computer, with capacity to handle a large number of connections. The nodes connect to this host computer are either terminals with little or no processing capabilities or microcomputers running special terminal emulation software such as Windows Remote Desktop.

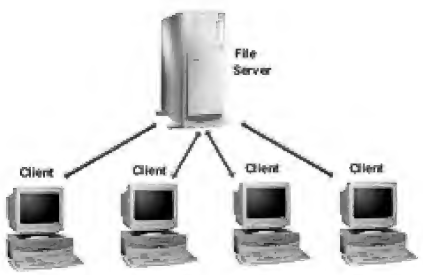


Figure 16.27 Client Server

Client Server

Client/server networks use central computers to

coordinate and supply services to other nodes on the network. The server provides access to resources such as Web page, databases, application software, and hard ware. Server nodes request the services.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations.

P2P (Peer to Peer)

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads among peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

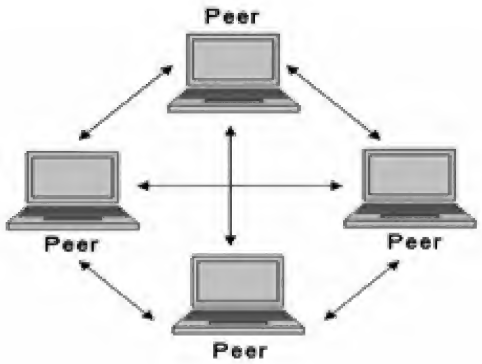


Figure 16.28 Peer to Peer

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply (send), and clients consume (receive).

Peer-to-peer networks are generally simpler, but their performance usually decreases when there is heavy load.

A summary is shared below for quick reference of various network strategies:-

Strategy	Summary Description
Terminal	✓ Centralized processing power, location, and control. ✓ Underutilized processing power of microcomputers.
Client/server	✓ Client request services. ✓ Servers provide services and coordination. ✓ Efficient network management software. ✓ Expensive.
Peer-to-peer	✓ All nodes act as clients and servers. ✓ Easy and inexpensive. ✓ Lacks security controls.

Table 16.1 Network Strategies

USEFUL TIP

Nowadays a P2P based file sharing application called Bit Torrents is very popular among youngsters for sharing Movies/Songs.

QUICK REVIEW

- What are the various kinds of Network Strategies?
- What is the difference between Client Server & P2P (Peer to Peer) models?

wide range of different network configurations, operating systems & strategies. Integrating or connecting all of these networks is a big task.

16.2.6 Organizational Scope

The various types of Internet technologies which are deployed by organizations are enlisted below:-

1. **Intranet** –
   It is simply the organization's own private Internet version.
2. **Extranet** –
   It is a private network that connects more than one organization. It functionally provides outside access to an organizational Intranet.

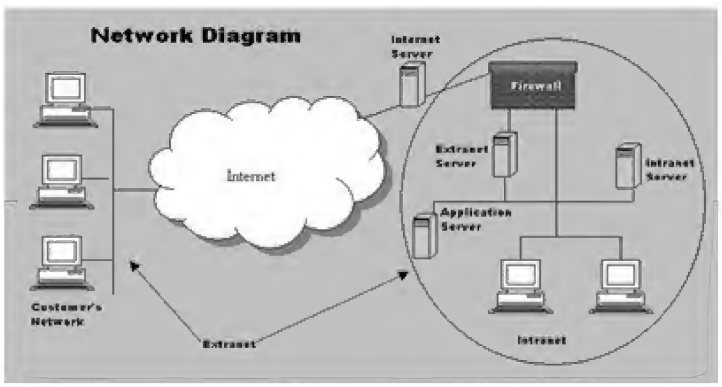


Figure 16.29 – Intranet & Extranet

3. **Firewall** –
   It is a special security system designed to protect an organization's network against external threats. It consists of hardware and software that control access to a company's intranet or other internal networks.

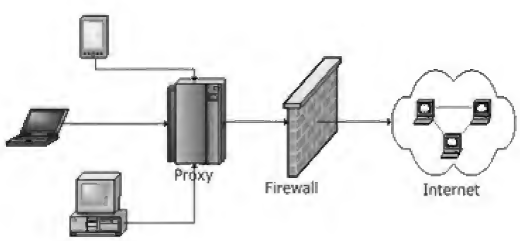


Figure 16.30 - Firewall

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

USEFUL TIP

Firewall is very critical in protecting a company's vital information assets. It may be used as a software or hardware

QUICK REVIEW

- What are the various kinds of Organizational level network structures?
- What is the difference between Intranet & Extranet?

16.2.7 Network Bandwidth Classification – Transmission Channels

A transmission/communication channel is the link or path between sender & receiver. Following are major categories:

Narrow Band

These channels range in speed from 45-300 bps (bits per sec). This channel is mainly used for telegraph line and low speed terminals.

Voice Band

These channels can transmit data at speeds up to 9600 bps. Its main use is in ordinary telephone voice communication.

Broad Band/Wide Band

These are used when large volumes of data are to be transmitted at high speed. Data transmission rate of this channel is 1 million bps or more. These channels are used for high speed computer to computer data communication. e.g. Cable TV, DSL & Fiber Optic.

16.3 Uses of Computer Networking

The main benefits or uses of computer network are:

Communication

Between individual communications is one of the biggest advantages provided by the computer networks. Different computer networking technology has improved the way of communications; people from the same or different organization can communicate in minutes for collaborating work activities. In offices and organizations computer networks are serving as the backbone of the daily communication.

Sharing Resources

In a computer network, resources such as, printers, scanners, fax machines and modems can be shared among different users.

Sharing Software

In a computer network, usually application programs and other software are stored on the central computer. Users connected to a network can access these softwares.

Data sharing

Another wonderful advantage of computer networks is the data sharing. All the data such as documents, file, accounts information, reports & multimedia etc. can be shared with the help computer networks.

Centralized Support & Administration

Computer networking centralizes support, administration and network support tasks. Technical personnel manage all the nodes of the network, provide assistance, and troubleshoot network hardware and software errors. Network administrators ensure data integrity and devise systems to maintain the reliability of information through the network. Unlike a stand-alone system, a networked computer is fully managed and administered by a centralized server, which accepts all user requests and services them as required.

USEFUL TIP

Communication is best use of Networking. Internet is the biggest example of Computer Network.

QUICK REVIEW

- What are the uses of Computer Networking?
- How can you share a Printer among 2 computer users?

16.4 Network Security Issues

Security over the Internet and over various Networks is becoming a very serious concern at this point since an increasing amount of information is traversing many more points of access. The stage is thus set for unbelievable information sharing on both levels and so the need for network security is paramount to prevent against countless threats.

- **Security**is the ability of a system to protect information and system resources with respect to confidentiality and integrity.

- **Confidentiality**: Ensuring that information is not accessed by unauthorized persons.
- **Integrity**: Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users

Types and Sources of Network Threat

Attacks are often maliciously used to consume and destroy the resources of a network. In order to properly identify and deal with probable threats, one must be equipped with the right tools and security mechanisms.

Attacks are generally classified into two types:

a**) Passive Attacks**: Passive attacks are those attacks in which the attacker's main aim is to obtain the information which is passing over the network. In this the attackers does not modify the content.

b) **Active Attacks**: It is just opposite to Passive attacks. In this the Attacker modifies the original message in some manner. The content of the original message is modified and then the modified message passes over the network.

Security risks to home users

The home computer user is often said to be the weakest link in computer security. They do not always follow security advice, and they take actions which leads there trap into threats that compromise themselves.

There are a number of pieces of malicious code spreading on the Internet through email attachments, known as software vulnerabilities.

Information security is concerned with 3 main areas:

1. **Confidentiality** - Information should be available only to those who rightfully have access to it. Loss of confidentiality is known as interception.
2. **Integrity** - Information should be modified only by those who are authorized to do so. Loss of Integrity is called Modification.
3. **Authentication** - It helps to prove the identity of the Sender. It ensures that the origin of an electronic message or document is correctly identified. Absence of Authentication is called Fabrication.

The most common methods used by hackers to gain control of home computers are:- Trojan horse programs, Back door and remote administration programs, Denial of service, , Unprotected Windows shares, Mobile code, Cross-site scripting, Email spoofing, Email borne viruses, Chat

clients, Packet sniffing etc.

USEFUL TIP

Tip: In order to ensure good Network Security, a Firewall along with Anti-Virus/Anti Malware application must be used. Prevention is always better than cure.

QUICK REVIEW

- What are the types of Security Attacks on a Network?
- What are the 3 concern areas of Information Security?

16.5 Software & Hardware Issues in Networking

A network is defined as a group (2 or more) of systems such as Windows desktop and server platforms that connect together for the purpose of sharing resources. Networks are used to give centralized access (secure access) to networked resources and generally, the entire network (whether it be a home based office, or a corporation's infrastructure) all connect up to the biggest shared resource in use today – the World Wide Web.

Few major issues are discussed in detail below:

Initial Configuration

The first problem that comes to mind is glitches that occur when configuring your network, your systems and resources for use. There are many components to a typical network and as size and use grows, so do its complexities and the possibility for problems to arise. There are various ways of doing things, and so, the best practices should be considered and followed.

When setting up your systems, the biggest things that cause disruption are loss of your main power source, incorrect cabling (or wireless configurations), lack of/or misconfigured protocols (such as IP) and problems with Windows systems such as misconfigured network services.

Credential, Permission and Rights Problems

Most times, you may try to access a host and not be able to because they cannot log in, or they do not have permissions to access resources once they are logged in. Usually, someone knowledgeable in this area (a systems or network administrator, for example) may have configured this for you. If you did it yourself, you really need to have a check on password/credential logs.

Network Performance

This is by far the most common issue with networking in general. If network performance is

impacted, either the network is too slow (very common term), or the application was not developed with the network in mind. It can be confusing to solve this type of issue and normally requires advanced analysis of the problem to solve.

Speed and Latency issues can be the result of slow connections, or from a network that is saturated with data. Also, using a hub instead of a network switch (that keeps a switching table in memory) can cause major issues with speed and latency.

Other issues that relate to performance are security that tie up your systems resource, or purposely cause your services to fail.

Internet browsers can also cause an issue (especially if they are infected with a virus) so make sure that this is not the case, or that your systems browser settings are not restricting sites.

TCP/IP and other Protocol Problems

Here are many reasons why this can be an issue, to name a few – ISP-based protocol issues, DHCP, DNS, IP addressing and/or using a different protocol suite other than TCP/IP within your network. You can solve most of your TCP/IP related problems by having an updated document of your topology, even if it is a few systems. Being able to view a graphic is extremely helpful when trying to resolve a network issue, or, to quickly add a new host to your network without causing an issue.

At a high level (usually corporate networks), IP packets are routed over multiple devices and links which takes the problem (packet loss) and multiplies it times the amount of gear you are using.

General Security Concerns

The biggest networking issue when dealing with Windows based network clients is the poor application of basic security services and features or lack thereof.

It is a fact that most of the intrusions over your network come from within the network, or very easily over wireless connections. This is seen more so with home offices and small companies that cannot afford (or are oblivious to) enterprise security solutions used to control, monitor and lock down wireless usage. That does not mean that your home PC, or router cannot be '**secured**'. The benefits you get from most hardware and software sold today is that almost everything you get now comes with good level of security features.

Routers are now firewalls, IDS (intrusion detection systems), and provide detailed logs of everything going through it. It should be mentioned that applying wireless security is not simple; to secure a wireless network is to use MAC addresses of the clients in your office that are on a list the access point maintains so that only those users have access.

Whether using the Windows Firewall, or some other third party software offering, you should always consider using one as the most basic form of host protection.

Network based intrusion detectors can help trend data and lock down anything that seems 'fishy'. The router you use may have firewall capabilities, amongst other things (VPN/Encryption), IDS, Wireless AP with security features. Antivirus (can be used to reduce connectivity and performance issues. Most viruses today (as well as worms) operate to do the host system, or network harm.

The most important thing you should take away from this biggest problem (or concern) is that security when applied needs to be tested and then monitored continuously.

USEFUL TIP

To keep your Network issues down, one needs to periodically monitor, evaluate and test the settings. It is an ongoing process and needs good knowledge of computer know how.

QUICK REVIEW

- What are the various kinds of Network Issues?
- Which is the biggest Network Issue & how can we tackle it?

Multiple Choice Questions

1. Which of the following is not a physical network link

   a. Twisted Pair b. Coaxial Cable

   c. Optical Fiber d. Optical Disk

2. Which of the following is not a type of network topology:

   a. Bus b. Tree

   c. Ring d. Circle

3. In computer network, nodes are

   a. the computer that originates the data

   b. the computer that routes the data

   c. the computer that terminates the data

   d. all of the mentioned

4. Communication channel is shared by all the machines on the network in

   a. broadcast network

   b. unicast network

   c. multicast network

   d. none of the mentioned

5. Bluetooth is an example of

   a. personal area network

   b. local area network

   c. virtual private network

   d. none of the mentioned

6. A _____ is a device that forwards packets between networks by processing the routing information included in the packet.

   a. bridge

   b. firewall

   c. router

   d. all of the mentioned

7. Which of the following is not a type of Network

   a. MAN b. TAN

   c. PAN d. WAN

8. Network congestion occurs

   a. in case of traffic overloading

   b. when a system terminates

   c. when connection between two nodes terminates

   d. none of the mentioned

9. Which is the full form of BAN?

   a. Body Area Network

   b. Best Area Network

   c. Boost Area Network

   d. None of the above

10. Which is not a type of network topology?

    a. Star b. Ring

    c. Mesh d. Hexagon